CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

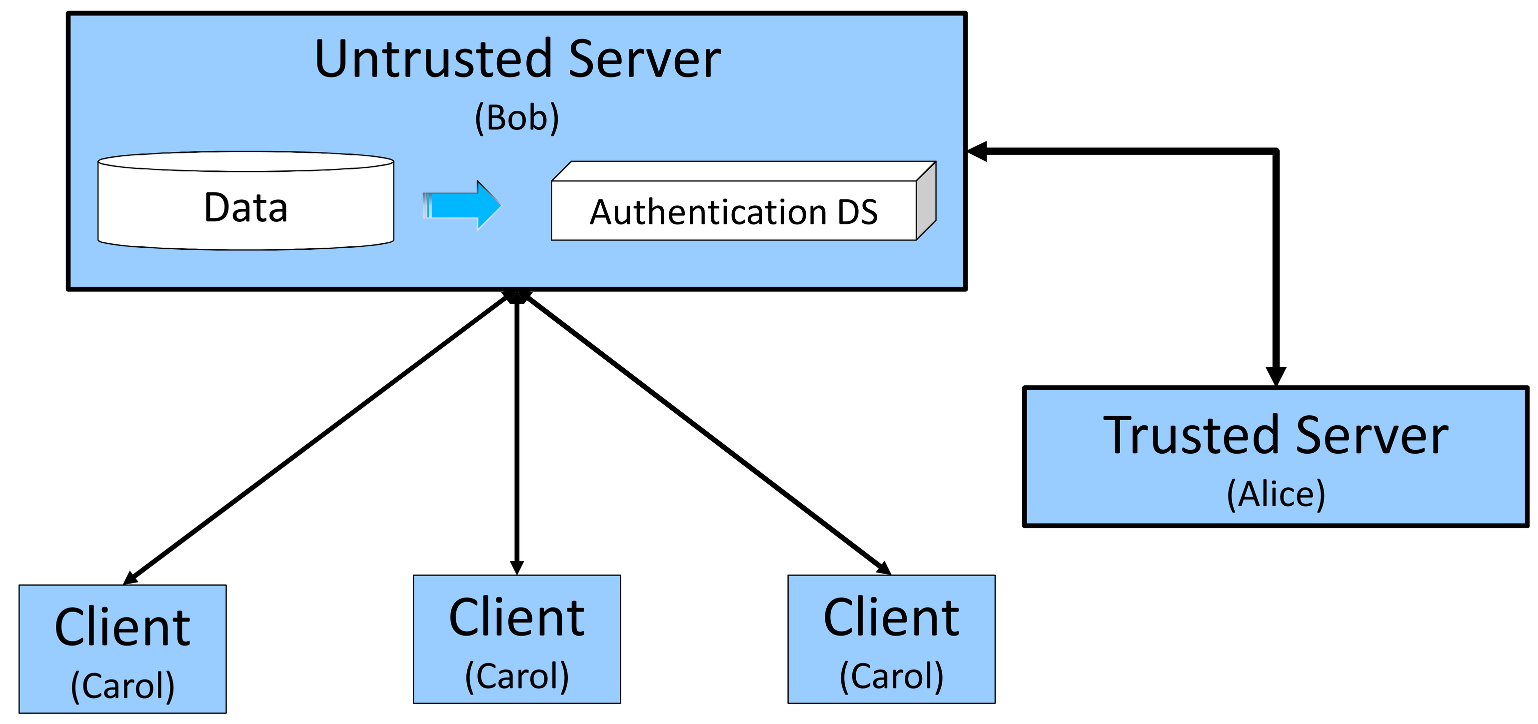
Trustworthy Data From Untrusted Databases

Rohit Jain, Sunil Prabhakar
{jain29, sunil}@cs.purdue.edu
Purdue University

Motivation

- Data is often stored at untrusted servers
  - Data in the cloud
  - Insecure server
- Can we establish the trustworthiness of data from these servers? I.e. :
  - Authenticity of retrievals
  - Integrity of data (updates)
  - Secure provenance of data
  - Indemnity for the server (cloud)

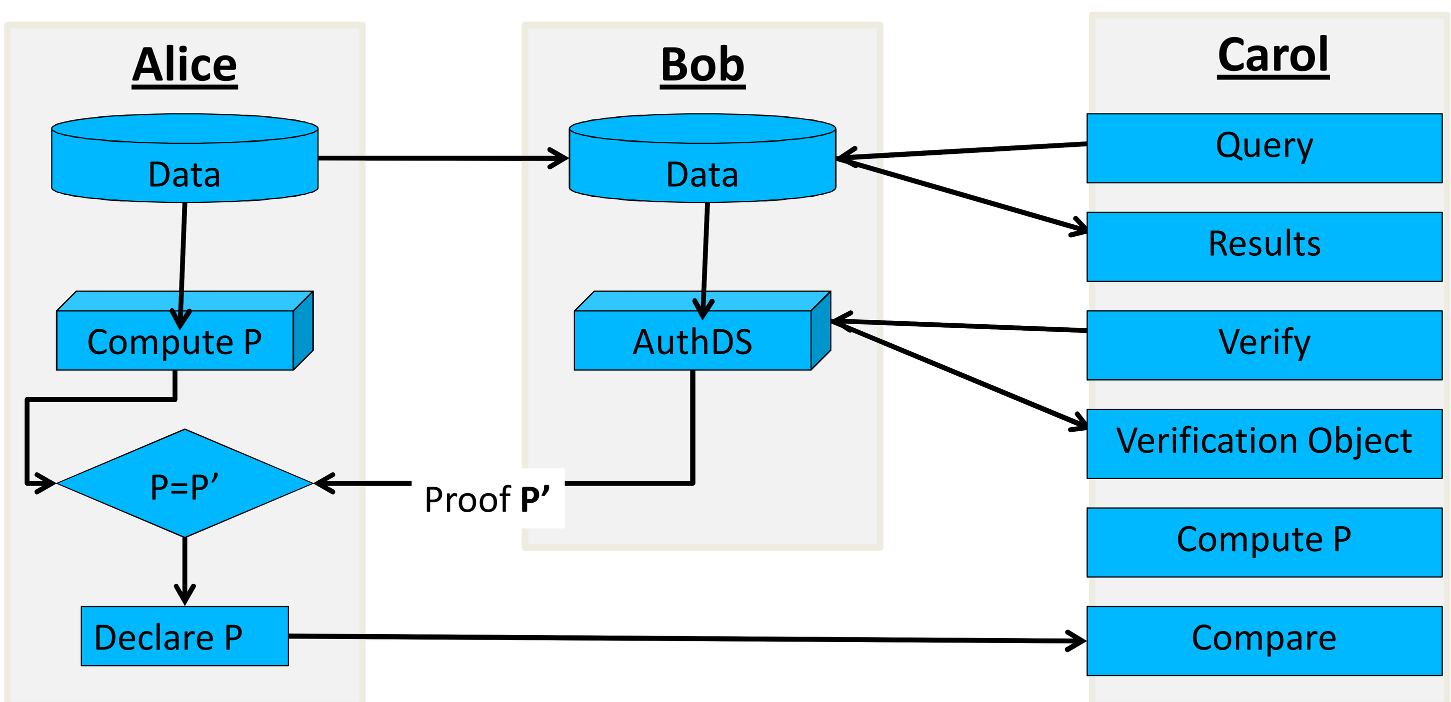
Model



Protocol for Static Data

Data is static

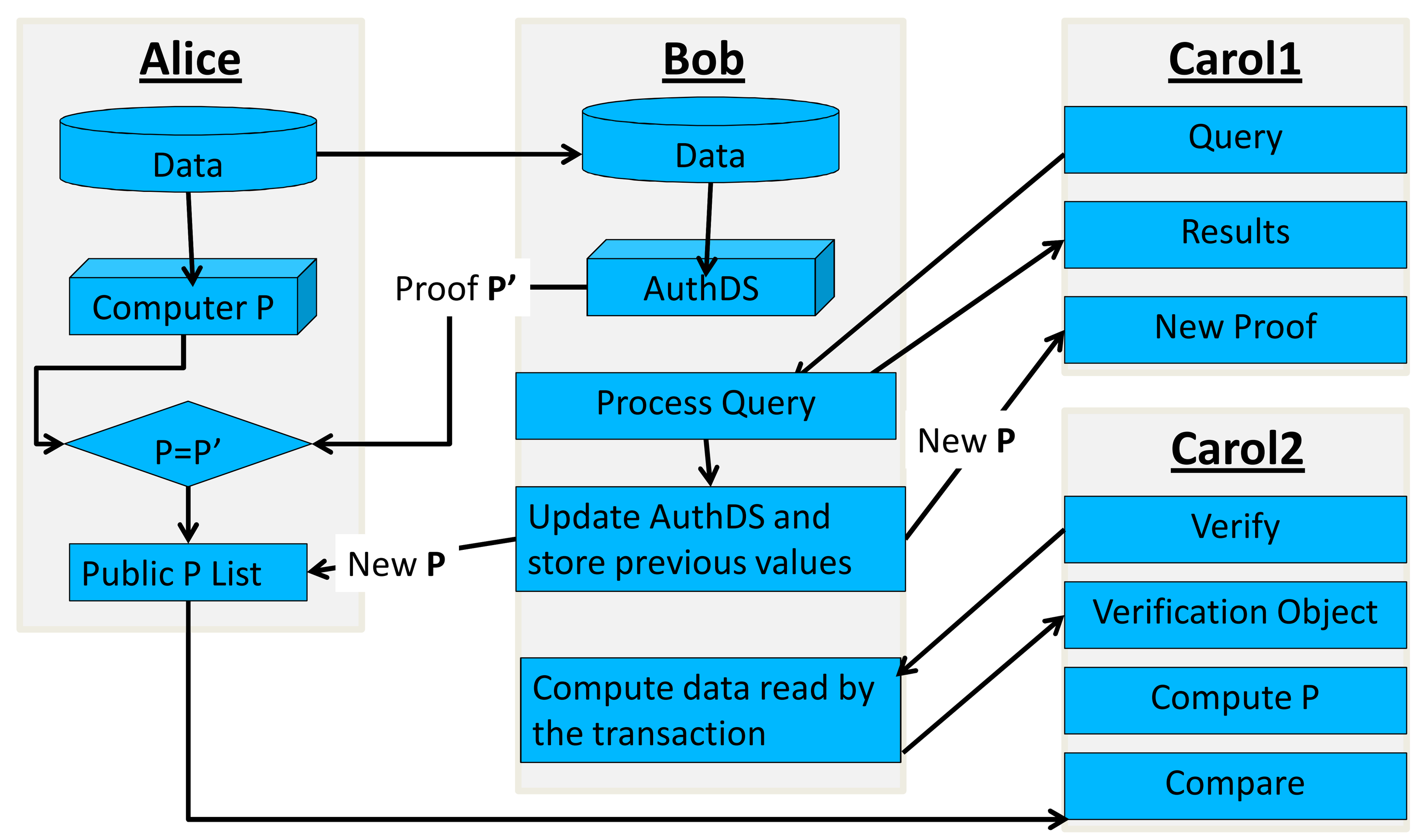
- Only Alice can modify data



Challenge : Dynamic Data

Clients can modify data. No centralized vetting of updates

- A trusted server is used to keep track of *proofs*



Experiments

Easy to implement on top of an existing DBMS (e.g. Oracle)

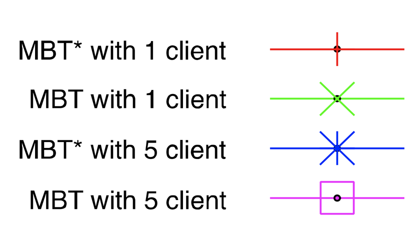


Fig 1: Legends

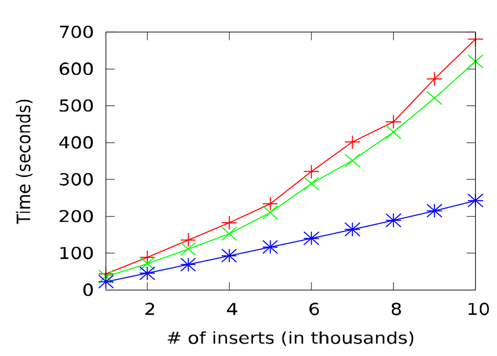


Fig 2: Insert Time

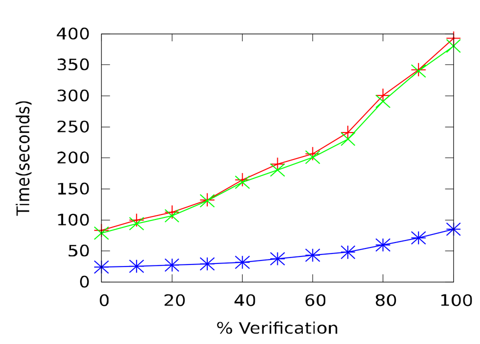


Fig 3: Insert + Verification Time

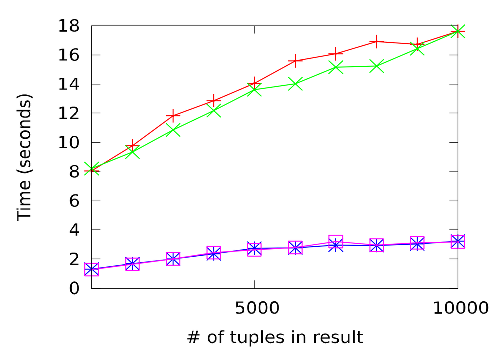


Fig 4: Search + Verification Time

Conclusion

- Protocols provide authenticity, integrity and indemnity for relational databases
- Significantly reduces level of trust required
- Provides secure provenance of data
- Verification is decoupled from transaction execution
- Easy to implement and reasonable overhead

CERIAS

Discovery Park
e-Enterprise Center